кумента (в частности, это относится и к MathML). В-третьих, распространяется этот браузер в исходных кодах и его можно свободно скачивать с сайта W3C. Наконец, в нем реализована технология CSS и поддержка XHTML. Его главным недостатком, на мой взгляд, является большое количество ошибок. Стоит, однако, заметить, что проект, разрабатываемый в стиле базар, вполне может преодолеть эти трудности за счет работы энтузиастов. Что же касается реализации MathML, то здесь, по-видимому, просто еще слишком много недоделок.

Вот пример математики, отображенной Amaya:

$$E_s(\omega_s) = \frac{r_e e^{ik_s x}}{2\pi x} \int T \kappa \overleftrightarrow{\Pi} \cdot E_i e^{i(\omega t' - k \cdot r')} dt' \qquad (5.2)$$

В заключение еще раз подчеркнем, что MathML появился относительно недавно и находится в стадии становления. Нельзя исключить того, что через несколько лет MathML уступит место более мощной и совершенной технологии. Однако уже сейчас можно с уверенностью сказать, что глубокие идеи, заложенные в этот язык, послужат прочной основой для создания будущих методов представления сложных научно-технических документов.

В эпоху развития интернет-технологий остро возник вопрос о создании сайтов со специфическим содержанием, то есть содержащим особую разметку, и специфические изображения.

**С. В. Ченушкина, гр. КТ-501**

## ВЛИЯНИЕ ЧЕЛОВЕЧЕСКОГО ФАКТОРА НА ПРОЦЕСС ПРОЕКТИРОВАНИЯ И ВНЕДРЕНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Любая система начинается с модели: макета, образца, прототипа или просто не воплощенного мысленного образа. При его построении стараются учитывать максимальное количество влияющих на систему факторов риска: связи, ситуации, давление со стороны других систем, внутренние связи. Все слабые и сильные стороны будущей системы. Проектировщики теряют огром-

ное количество времени на анализ систем выявления их достоинств, недостатков, прежде чем приступят к творению.

И когда, казалось бы, всё предусмотрено, остается только начать воплощать идеи в жизнь, реализовывать модель, возникает несколько человеческих «НО».

Вот лишь несколько цитат:

- *«По данным Gartner Group, ущерб, связанный с ошибками персонала, а также с действиями обиженных и нечестных сотрудников, составляет более 70%».*[1]
- *«Психологическое неприятие системы IFS Applications некоторыми сотрудниками предприятия (хотя она довольно проста в эксплуатации)».*[2]
- *«Другие, к которым я обращался с предложениями о заполнении входных форм документов, обычно ссылались на нехватку времени».*[3]
- *«Неправильная сборка, установка, старые драйвера, неумелое использование программ, не сделанное вовремя обновление»*[4]
- *«На 2 минуте старта вырубилось питание (автономное) стартового компьютера и чипы выдавались несколько минут без регистрации», «перепутали номера станций, и программа начала снимать всех подряд участников у кого эти пункты были».*[5]

И это лишь вершина айсберга, под названием - **«Human factors»**, ***человеческий фактор*** - характеристики человека (или группы людей) и машины (или технические системы), проявляющиеся в конкретных условиях их взаимодействия в системе "человек - машина", функционирование которой определяется достижением поставленной цели.[6]

С другой стороны - систему тоже разрабатывает человек, он же составляет базу, программирует и внедряет. Неужели люди не смогут договориться между собой?

Рассмотрим на примере модели: заказчик-программист-пользователь.

Итак, **заказчик,** основной вопрос – «Что должно быть?».

Являясь постановщиком задачи и денежным эквивалентом продукта, абсолютно не ориентируется, в том «как это сделать» пытается направить программиста на результат или исправить положение. При этом для однозначного определения задачи, она изначально должна быть грамотно поставлена. Зачастую конечный продукт несколько отличается от требований заказчика, особенно в том случае, когда последний не следит за ходом деятельности.

**Программист**, основной вопрос – «Что делается?».

Это компьютерный рабочий, общается на компьютерном жаргоне, поэтому часто воспринимает заказ по-своему, заказчик же не всегда понимает программиста. Он определяет написание сметы по созданию продукта. Основное ***кредо***: создать максимально автоматизированную систему, позволяющую за минимальное время достичь поставленной цели. Отдельный вопрос дизайн, эргономичность. Здесь в цепочку вступает потенциальный пользователь.

**Пользователь,** куча вопросов: «Зачем это нужно? А что будет, если… А это, что за кнопочка? Что-то выглядит не очень».

При разработке берется во внимание потенциальный пользователь, который и задает все эти вопросы плюс удобство навигации, общедоступность информативность. Основная проблема - научить пользователя работать с системой, на этом этапе человеческий фактор оказывает огромное влияние: нехватка времени, боязнь компьютера, психологическое противостояние системе. Обычно в этом случае пользователи проходят этап подготовки: групповой или индивидуальный.

Чтобы система была работоспособной и нашла свое применение, необходимо, чтобы при создании модели подход к ней осуществлялся минимум с трех подходов: заказчика-программиста-пользователя.

Отдельный вопрос защита созданной системы. Все программные средства обеспечения безопасности и защиты от несанкционированного доступа, так или иначе, связаны с использованием паролей или других, связанных с ними, технологий.

Пароль играет ключевую роль в системе безопасности, а он, в свою очередь, всецело зависит от пользователя. Таким образом, человеческий фактор

непосредственно влияет на уровень безопасности автоматизированной информационной системы. Возможные ошибки пользователя [8]:

1. Неграмотное составление пароля.
2. Умышленная или неумышленная передача паролей третьим лицам.
3. Умышленная или неумышленная передача прав доступа третьим лицам.
4. Использование небезопасных средств передачи информации.
5. Использование непроверенного (ненадежного) программного обеспечения.
6. Заражение системы вирусами или другими неавторизованными программами-вкладками.
7. Хранение пароля на открытом месте: стикер на мониторе, записная книжка, надпись на руке или в памяти компьютера.

Можно сделать вывод, что человеческий фактор становится решающим, как на этапе внедрения информационной системы, так и при обеспечении её безопасности. Это подтверждает и статистика: в большинстве случаев пользователи умышленно или неумышленно помогают взломщикам, в 70% случаев сбои в работе информационных систем вызваны сотрудниками, т.е. человеческим фактором.

**Литература**

1. Александр Любинский: как защитить информационную систему от атак//http://www.aladdin.ru/press/articles/article343.php
2. Елена Шашенкова. Даже «Мерседесы» нельзя продавать без системы автоматизации http://iemag.ru/?ID=473265
3. В. Е. Кириенко. Человеческий фактор корпоративных информационных систем.
4. http://www.compass-ps.ru/Index.html
5. Большая советская энциклопедия // http://encycl.yandex.ru/
6. http://www.ibresource.ru/forums/lofiversion/index.php/t12963.htm

7. Климашевич С.Н. Безопасность в автоматизированных информационных системах. Человеческий фактор.// http://www.mstu.edu.ru/publish/conf/11ntk/section4/section4_18.html